



Εταιρική Διακυβέρνηση και Ασφάλεια Πληροφοριών

από τον **Νίκο Βασιλειάδη**
ISO 27001 & 9001 Auditor, CISA, CISM, CISSP, ISEB BCMP, HISP, MCSE

Το επιχειρείν ήταν πάντοτε και εξακολουθεί να είναι μια συνεχής διεργασία διαχείρισης κινδύνων και εκμετάλλευσης ευκαιριών. Οι δυο αυτές έννοιες είναι συνυφασμένες με την αβεβαιότητα και μέσα σε αυτές τις συνθήκες κάθε επιχείρηση προσπαθεί να επιτύχει τους στόχους της μέσα στους οποίους, και ειδικά στις δύσκολες εποχές που διανύουμε σήμερα, δεν μπορεί παρά να είναι και η διατήρηση της εμπιστοσύνης του επενδυτικού (και όχι μόνο) κοινού απέναντί της. Η εδραίωση αυτής της εμπιστοσύνης καθώς και η απρόσκοπτη επίτευξη των στόχων περνά απαραίτητα μέσα από τη χρηστή εταιρική διακυβέρνηση η οποία θα πρέπει να στηρίζεται σε σωστές βάσεις και οι αρχές της να διαχέονται στο σύνολο του προσωπικού.

Σε διεθνές επίπεδο το θέμα της εταιρικής διακυβέρνησης έχει διερευνηθεί διεξοδικά και έχει οδηγήσει σε μια σειρά κωδίκων και πλαισίων και στις δυο πλευρές του Ατλαντικού. Από την άλλη πλευρά, μια σειρά από δυσάρεστα συμβάντα στο διεθνή χώρο των επιχειρήσεων ανάγκασαν τις κυβερνήσεις να νομοθετήσουν σχετικά και να επιβάλουν τις αρχές της εταιρικής διακυβέρνησης στο σύγχρονο επιχειρείν. Προς αυτή την κατεύθυνση κινήθηκε και η Ευρωπαϊκή οδηγία **2006/46/EK** η οποία υποχρεώνει τις εταιρείες των οποίων οι μετοχές ή κινητές αξίες διαπραγματεύονται σε οργανωμένη αγορά να υποβάλουν μαζί με τα αποτελέσματά τους και δήλωση εταιρικής διακυβέρνησης. Η οδηγία αυτή ενσωματώθηκε πρόσφατα στην ελληνική έννομη τάξη με το **Ν.3873/2010**.

Η δήλωση εταιρικής διακυβέρνησης κατ'απαίτηση του νόμου θα πρέπει να περιλαμβάνει μεταξύ άλλων:

1. Αναφορά στον κώδικα εταιρικής διακυβέρνησης στον οποίον υπάγεται η εταιρεία ή τον οποίον έχει αποφασίσει αυτοβούλως να εφαρμόζει και τον τρόπο στον οποίο δημοσιοποιεί το σχετικό κείμενο.

ΣΕ ΑΥΤΟ ΤΟ «ΕΙΔΙΚΟ ΤΕΥΧΟΣ»:

- ▲ Εταιρική Διακυβέρνηση και Ασφάλεια Πληροφοριών
- ▲ Εσωτερικός Έλεγχος και Ασφάλεια Πληροφοριών
- ▲ Ανάλυση Κινδύνων και Δικλείδες Ασφαλείας
- ▲ Μετρήσεις και Διορθωτικές Ενέργειες

Εσωτερικός Έλεγχος και Ασφάλεια Πληροφοριών

Σε κάθε σύγχρονο οργανισμό, κερδοσκοπικό ή μη, υπάρχει μια ιεραρχία η οποία στη συντριπτική πλειοψηφία των περιπτώσεων έχει τη μορφή πυραμίδας με την έννοια ότι οι λίγοι διοικούν τους πολλούς. Το τμήμα της διοίκησης όμως είναι, ή τουλάχιστον πρέπει να είναι, η ευθύνη. Κάθε επιχείρηση έχει έναν ή περισσότερους νόμιμους εκπρόσωπους οι οποίοι και αναλαμβάνουν την ευθύνη σε περίπτωση που στελέχη της επιχείρησης προξενήσουν ζημιά ή για οποιοδήποτε λόγο οι πελάτες της δεν είναι ευχαριστημένοι. Η ευθύνη μάλιστα δεν είναι μόνο απέναντι στους πελάτες αλλά και απέναντι στους ιδιοκτήτες και μετόχους της επιχείρησης οι οποίοι πρέπει να ενημερώνονται επακριβώς για την πορεία της. Όταν μάλιστα η επιχείρηση είναι εισηγμένη σε δημόσια αγορά τότε η προστασία των συμφερόντων των μετόχων της αποτελεί θεσμική ανάγκη και θα πρέπει να υπηρετείται αναλόγως.

Εδώ όμως προβάλλει το σημαντικό ερώτημα: Πώς είναι δυνατόν η διοίκηση της επιχείρησης η οποία αρκετές φορές δεν είναι εξοικειωμένη με το καθαυτό αντικείμενό της να φέρει την ευθύνη για τις «πράξεις και παραλείψεις» της επιχείρησης; Πώς είναι δυνατόν για παράδειγμα ο διευθύνων σύμβουλος μιας εταιρείας επικοινωνιών να έχει την τεχνική γνώση για να παρακολουθήσει την ποιότητα των υπηρεσιών που παρέχει η εταιρεία στους πελάτες της ή τις γνώσεις λογιστικής που απαιτούνται για να διασφαλίσει ότι ενημερώνονται σωστά οι μέτοχοί της; Πώς με απλά λόγια είναι δυνατόν να καλύψουμε το κενό ανάμεσα στην κορυφή της πυραμίδας και τη βάση της; Αυτό το ρόλο παίζουν τα Συστήματα Εσωτερικού Ελέγχου, βασικό συστατικό της Εταιρικής Διακυβέρνησης. Σκοπός τους είναι να διατηρείται η πορεία της επιχείρησης μέσα στην πορεία επίτευξης των στόχων που έχει θέσει η διοίκηση, να γίνεται έγκαιρη και ορθή αποτίμηση των κινδύνων που απειλούν την επιχείρηση και να διασφαλίζεται η συμμόρφωσή της με τους νόμους και τις κανονιστικές διατάξεις στις οποίες υπάγεται.

Ποιο είναι το βασικό συστατικό της διεργασίας του Εσωτερικού Ελέγχου; Μα φυσικά η ορθή, απρόσκοπτη και ασφαλής διακίνηση και τήρηση των πληροφοριών είτε από την κορυφή προς τη βάση της πυραμίδας (εντολές διοίκησης) είτε από τη βάση προς την κορυφή της (ενημέρωση διοίκησης). Κάθε τμήμα της επιχείρησης, ακόμα και αν αυτή επιμένει παραδοσιακά και δεν υιοθετεί σύγχρονα πληροφοριακά συστήματα, παράγει μεγάλες ποσότητες πληροφοριών. Είτε οι πληροφορίες έχουν τη μορφή προσφορών, είτε οικονομικών καταστάσεων, είτε τιμοκαταλόγων η επιχείρηση οφείλει να τις διακινεί με κατάλληλο τρόπο και να γνωρίζει κάθε κίνδυνο ο οποίος απειλεί την ασφάλειά τους προκειμένου να τον αντιμετωπίσει. Από τη στιγμή που θα τεθεί σε κίνδυνο ή απλώς θα αμφισβητηθεί η ασφάλεια των πληροφοριών, το σύνολο του οικοδομήματος του Εσωτερικού Ελέγχου τίθεται σε κίνδυνο.

Ξέρετε ποιος βρίσκεται πίσω από την πρώτη πλατφόρμα λογισμικού για τη διαχείριση συστημάτων Ολικής Ποιότητας στην Ελλάδα;



www.msms.gr

Ανάλυση Κινδύνων και Δικλείδες Ασφαλείας

Ξεκινήσαμε με το ρόλο της αβεβαιότητας στο σύγχρονο επιχειρείν και αυτή την αντίληψη θα διατηρήσουμε μέχρι το τέλος. Οι κίνδυνοι που απειλούν τη δραστηριότητα μιας επιχείρησης είναι πάρα πολλοί και τις περισσότερες φορές είναι δύσκολο να τους εντοπίσουμε διότι ξεκινάμε με λάθος τρόπο. Είναι σχεδόν αδύνατο να αναγνωρίσει κανείς και να ποσοτικοποιήσει τον κίνδυνο που απειλεί μια ολόκληρη επιχειρησιακή διεργασία στην οποία συμμετέχουν άνθρωποι, μηχανές και υλικά. Η αναγνώριση και ποσοτικοποίηση του κινδύνου επιβάλλεται όμως προκειμένου να αποφασιστεί ο τρόπος αντιμετώπισής του.

Κατά την πρώτη φάση της ανάλυσης κινδύνων εντοπίζεται η εξάρτηση της κάθε επιχειρησιακής διεργασίας από τον εξοπλισμό και τα στελέχη του οργανισμού (από τα αγαθά δηλαδή που χρησιμοποιεί), ώστε να είναι κανείς σε θέση να κρίνει τη σημαντικότητα κάθε αγαθού (asset) και να καταγράψει τους κινδύνους που το απειλούν. Είναι πολύ πιο εύκολο να καταγράψει κανείς τους κινδύνους που απειλούν μια συγκεκριμένη μηχανή στην οποία εκτελείται το MIS της επιχείρησης παρά να καταγράψει τους κινδύνους που απειλούν τη διεργασία παραγωγοληψίας. Συνεπώς η αποτύπωση αυτής της εξάρτησης και της συμβολής του κάθε asset στις επιχειρησιακές διεργασίες είναι κεφαλαιώδους σημασίας και απαιτεί βεβαίως πολύ καλή γνώση της μηχανογραφικής υποδομής και της λειτουργίας της επιχείρησης.

Εφόσον καταγραφούν και αξιολογηθούν οι κίνδυνοι το επόμενο βήμα είναι η απόφαση σχετικά με τον τρόπο αντιμετώπισής τους. Οι επιλογές είναι συνήθως τέσσερις: Αντιμέτωπιση του κινδύνου με στόχο τη μείωση των επιπτώσεων ή της πιθανότητας εκδήλωσής του, μεταφορά του σε κάποιον άλλον που πληρώνεται για να τον αναλάβει όπως π.χ. μια ασφαλιστική εταιρεία, αποφυγή του ακυρώνοντας τη διεργασία που τον περιλαμβάνει και αποδοχή του στην περίπτωση που το κόστος αντιμετώπισης είναι δυσθεώρητο ή η αντιμετώπισή του εντελώς αδύνατη. Το ποια οδός θα ακολουθηθεί σε κάθε περίπτωση είναι απόφαση της διοίκησης η οποία θα ζυγίσει τα υπέρ και τα κατά και θα προχωρήσει στην υλοποίηση των απαραίτητων δικλείδων ασφαλείας. Οι δικλείδες ασφαλείας που θα επιλεγούν βέβαια είναι απαραίτητο να αντιμετωπίζουν επαρκώς τον κίνδυνο, να συνάδουν με την επίτευξη των στόχων της επιχείρησης και να είναι σύμφωνες με το νομοθετικό και κανονιστικό

πλαίσιο. Ο ρόλος του Εσωτερικού Ελέγχου λοιπόν που είναι επιφορτισμένος με τα παραπάνω είναι καθοριστικός και είναι υποχρεωμένος να ενημερώσει τη διοίκηση για τυχόν «εσφαλμένες» επιλογές δικλείδων ασφαλείας. Θα πρέπει να τονίσουμε προς κάθε δυνατή κατεύθυνση ότι είναι λάθος η πραγματοποίηση επενδύσεων σε μέτρα ασφαλείας και η εγκατάσταση εφαρμογών και μηχανών χωρίς την πρότερη αξιολόγηση των κινδύνων που καλούμαστε να αντιμετωπίσουμε.

Όλα τα παραπάνω εντάσσονται στα πλαίσια σύγχρονων προτύπων διακυβέρνησης πληροφορικής και ειδικότερα για το θέμα της ασφάλειας πληροφοριών η συμμόρφωση κάθε εισηγμένης εταιρείας με το ISO/IEC 27001:2005 πρέπει να θεωρείται επιβεβλημένη. Εκτεταμένη ανάπτυξη της μεθοδολογίας που προτείνουμε για το θέμα μπορεί ο αναγνώστης να βρει στο <http://www.securenews.gr>.



Ξέρετε ποιος βρίσκεται πίσω από τα περισσότερα πιστοποιημένα Συστήματα Διαχείρισης Επιχειρησιακής Συνέχειας στην Ελλάδα;



www.bs25999.gr

Μετρήσεις και Διορθωτικές Ενέργειες

Θα πρέπει να έχουμε κατά νου ότι οι ασφαλιστικές δικλείδες που επιλέγουμε και τα συστήματα που εφαρμόζουμε δεν μπορεί να είναι στατικά. Καθώς εξελίσσεται η τεχνολογία είναι επιβεβλημένο να εξελίσσονται και οι τρόποι που αντιμετωπίζουμε την αβεβαιότητα που αναφέρουμε στην εισαγωγή του πονήματος αυτού. Προκειμένου όμως να είμαστε βέβαιοι ότι αντιμετωπίζουμε τον όποιο κίνδυνο με τον ενδεδειγμένο τρόπο και ότι η επένδυσή μας στην ασφάλεια αποδίδει θα πρέπει να είμαστε σε θέση να μετρήσουμε αυτή την απόδοση. Το κακό δυστυχώς με την ασφάλεια είναι ότι ενώ οι δαπάνες γι' αυτήν είναι προφανείς, τα οφέλη από αυτήν είναι δύσκολο να διακριθούν και άρα να αποτιμηθούν. Η αρνητική προσέγγιση είναι συνήθως ο ενδεδειγμένος τρόπος: Τι θα κόστιζε στην εταιρεία αν διέρρεαν σημαντικές πληροφορίες για ένα καινούριο προϊόν; Ποιο θα ήταν το κόστος ενός προστίμου για τη μη συμμόρφωση και ποια η βλάβη στην εικόνα της εταιρείας; Θα ήταν ασφαλές να λέγαμε ότι οι απαντήσεις στα παραπάνω ερωτήματα αποτελούν το όφελος που απολαμβάνουμε επειδή ακριβώς παίρνουμε τα μέτρα μας για να μη συμβούν αυτά που περιγράφουν και άρα το όφελος των ασφαλιστικών δικλείδων που εφαρμόζουμε γι' αυτό. Το όφελος λοιπόν μιας ασφαλιστικής δικλείδας είναι το μέγεθος του κινδύνου που αντιμετωπίζει.

Είναι απαραίτητο βέβαια να έχουμε ένα μέτρο σύγκρισης προκειμένου να κρίνουμε αν οι επενδύσεις που έχουμε κάνει και τα μέτρα που έχουμε πάρει αποδίδουν ικανοποιητικά. Η βάση πάνω από την οποία πρέπει να βρισκόμαστε ορίζεται φυσικά από τη νομοθεσία. Η προστασία των ευαίσθητων προσωπικών δεδομένων π.χ. είναι κάτι που δεν μπορεί να αγνοηθεί από καμία επιχείρηση ακόμα κι αν το κόστος είναι μεγάλο. Είναι όμως κοινό μυστικό ότι στο σύγχρονο επιχειρείν δεν έχει τόσο σημασία η βάση όσο η οροφή και πόσο απέχουν οι άλλοι από αυτήν. Θα πρέπει λοιπόν να είμαστε σε θέση να συγκρίνουμε τα μέτρα ασφαλείας της δικής μας επιχείρησης με τους άλλους και να αποφασίσουμε για το αν μπορούμε και αν θέλουμε να πάμε παραπάνω. Αυτή η διεργασία (benchmarking) επιβάλλεται να γίνει από ειδικούς οι οποίοι θα μας βοηθήσουν να κάνουμε τις απαραίτητες διορθωτικές ενέργειες για να βρεθούμε στη σωστή κατεύθυνση.

Σε αυτό το σημείο ο ρόλος των επαγγελματικών ενώσεων όπως ο ΣΕΒ είναι καθοριστικός και αυτό ακριβώς αποτελεί την πρόταση του υπογράφοντος για το επόμενο βήμα: Τη διευκόλυνση της διαδικασίας του benchmarking με τη συλλογή και την επεξεργασία δεδομένων από κάθετες αγορές προκειμένου να υπάρχει μια εθνική βάση σύγκρισης. Είμαστε πρόθυμοι να βοηθήσουμε προς αυτή την κατεύθυνση.

Σχολιάστε

► ...συνέχεια

Εταιρική Διακυβέρνηση και Ασφάλεια Πληροφοριών

2. Αναφορά στις πρακτικές εταιρικής διακυβέρνησης που εφαρμόζει η εταιρεία επιπλέον του νόμου και παραπομπή στο διαδικτυακό τόπο όπου τις έχει δημοσιοποιήσει.

3. Περιγραφή των κύριων χαρακτηριστικών των συστημάτων εσωτερικού ελέγχου και διαχείρισης κινδύνων της εταιρείας σε σχέση με τη διαδικασία σύνταξης των χρηματοοικονομικών καταστάσεων.

Στα πλαίσια των παραπάνω αποκτά ιδιαίτερη σημασία /ενδιαφέρον η πρόσφατη ολοκλήρωση του **Κώδικα Εταιρικής Διακυβέρνησης** του ΣΕΒ για τις Εισηγμένες Εταιρείες (βλ. σχετικά στην ιστοσελίδα www.sev.org.gr), ο οποίος αποτελεί μια πλήρη και συγκροτημένη προσέγγιση του θέματος από τον ΣΕΒ και μπορεί να χρησιμοποιηθεί από τις εισηγμένες προκειμένου, μεταξύ των άλλων, να ανταποκριθούν στις νομοθετικές απαιτήσεις.

Δεν θα αναφερθώ εδώ στην ανάγκη ορθής εταιρικής διακυβέρνησης αγαπητοί αναγνώστες διότι το θέμα έχει **αναπτυχθεί επαρκώς** από τους άμεσα ενδιαφερόμενους και έχει **αξιολογηθεί** από ειδικούς. Δική μας δουλειά είναι να τονίσουμε το ρόλο των πληροφοριακών συστημάτων στην υπόθεση της εταιρικής διακυβέρνησης και να συσχετίσουμε τα θέματα της IT συμμόρφωσης γενικότερα με αυτήν.